# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

**4,800**
Open access books available

**122,000**
International authors and editors

**135M**
Downloads

Our authors are among the

**154**
Countries delivered to

**TOP 1%**
most cited scientists

**12.2%**
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

## Interested in publishing with us?
## Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

# 9

# Quantum Cryptography

W. Chen[1], H.-W. Li[1, 2], S. Wang[1], Z.-Q. Yin[1],
Z. Zhou[1], Y.-H. Li[3], Z.-F. Han[1] and G.C. Guo[1]
[1]*Key Lab of Quantum Information, CAS, University of Science and Technology of China,*
[2]*Zhengzhou Information Science and Technology Institute,*
[3]*Depart. of Elect. Eng. and Info. Sci., University of Science and Technology of China*
*China*

## 1. Introduction

Information protection has been an important part of human life from ancient time. In computer society, information security becomes more and more important for humanity and new technologies are emerging in an endless stream. Cryptography or cryptology is a technology to convert the information from readable state into nonsense, or do the contrary transformation. Information transmission and storage can be effectively protected by cryptography. Modern cryptography has been rapidly developed since World War II, along with the fast progress of electronics and computer science. Symmetric-key cryptography and public-key cryptography are two major fields of modern cryptography, depending on if encryption and decryption keys are same or not. One of the symmetric encryption algorithms named one-time pad (OTP) has been proven to be impossible to crack no matter how powerful the computing power is (Shannon, 1949), however, to generate and distribute the true random key steam the same size as the plaintext is a rigorous requirement. Quantum cryptography can provide a secure approach to exchange keys between legitimate users and can be used with OTP to fulfill secure communication sessions. The concept of quantum cryptography was originally proposed by Wiesner in 1960s (Wiesner, 1983), though its real development should be recorded from the first quantum key distribution (QKD) protocol presented by Bennett and Brassard in 1984 (Bennett, & Brassard, 1984). The research fields of quantum cryptography are wider than QKD, including quantum secret sharing , quantum authentication, quantum signature and so on. QKD is a major aspect of quantum cryptography and will be the only topic discussed in this chapter. Unlike public-key cryptography, the security of QKD is guaranteed by quantum mechanics rather than computational complexity. The most important property of QKD is to detect the presence of the behavior to intercept the key information illegally. The single photon used in QKD cannot be divided into smaller parts, which means the eavesdropper cannot hold a part of the particle then measure it. The eavesdropper cannot precisely duplicate a particle with the same quantum state as the original one unknown to her due to the quantum no-cloning theorem. To measure an unknown quantum system will cause it to "collapse" from a range of possibilities into one of its eigenstates. This character, together with the uncertainty principle, ensure the eavesdropper cannot get total information without disturbing the original quantum system.

In this chapter, a short summary of research status of quantum cryptography and the workflow of BB84 protocol is introduced. Then, the security of QKD is discussed and some aspects of practical QKD system are focused on. In section 3, the implementation technolgies of a secure and stable point-to-point QKD system and QKD network are presented. Some field QKD network experiments and their results will be shown in this section. Another section will discuss some technical and non-technical aspects of the applications of QKD. Finally, a short conclusion aiming at the future trends of QKD is proposed.

### 1.1 The research status of quantum cryptography

The first QKD experiment was implemented by Bennett and Smolin in 1989 (Bennett, et al., 1992) which opened the gate to real-life QKD. According to the implementation scheme of QKD protocol, there are discrete variable, continuous variable and distributed phase reference coding. According to the physical carrier of quantum information, there are polarization encoding, phase encoding, frequency encoding , amplitude encoding and so on. Free-space QKD and fiber QKD can be used as the quantum channel for photon-based QKD. Implementation scheme should be selected according to the channel character, the performance requirements, the operating condition and so on.

Fiber is the most widely used quantum channel, in which the polariztion and the phase encoding QKD schemes can be applied. Polarization encoding QKD schemes use the polarization states of photons to carry key information. Due to the intrinsic birefringence effect in fiber, the polarization states of photons are vulnerable to be interfered, which affects the polarization encoding rather than the phase encoding QKD system in common situation. Although there are some valuable polarization encoding QKD schemes (Ma, et al., 2008; Liu, et al., 2010), phase encoding QKD is still the major scheme used in fiber quantum channel. The encoder and decoder of phase encoding QKD system generally implemented with interferometer, which need to be precisely modulated and adjusted to meet the interference conditions. Some mature phase encoding systems based on different interferomter structures (Ribordy, et al., 1998; Gobby, et al., 2004; Mo, et al., 2005) have been proposed. At present, several experiments in fiber over 100Km (Gobby, et al., 2004; Mo, et al., 2005; Takesue, et al., 2007; Rosenberg et al., 2009; Stucki, 2009; Liu, et. al., 2010) and pulse repetition rate of 10 GHz have been reported (Takesue, et al., 2007). Although fiber is a good media to transmit photons and convenient to be integrated with existing optical communication network, the attenuation of the channel and the performance of practical device still limit the secure key distribution distance. Free space QKD, especially satellite to ground QKD is an available method to build a global secure communication network (Hughes, et al., 2002; Rarity, et al., 2002). Nowadays, a 144 Km free space QKD link has been implemented (Schmitt-Manderbach, et al., 2007) and more experiments aiming to satellite QKD are still in progress (Hughes & Nordholt, 2011).

A lot of countries, including the United State, European Union, Japanese, and China, have spent a lot to develop QKD technology, and some world famous project DARPA and SECOQC were executed. The 973 Program and 863 program of China have funded to support the QKD research from the 1990s. Some companies of quantum technology, such as ID Quantique in Swiss, MaigQ in US and Qasky in China, have been set up, and QKD systems for both education evaluation and telecom communication have been marketed.

### 1.2 BB84 protocol

QKD protocol is the agreement of particle preparation, information modulation, signal detection and detection results processing, which should be obeyed by communication parties in the key distribution sessions. QKD protocols can be divided into two major categories – preparation and measurement protocols and entanglement based protocols. The first and the most practical implemented QKD protocol, well known as BB84, was originally presented with photon polarization. In fact, any two pairs of conjugate states can be used to implement the protocol, such as the phase of a photon. The flow of BB84 can be described using photon polarization as following, where transmitter named Alice and receiver named Bob:

1. Information Agreement – Alice and Bob make agreements on the correspondence between quantum states and classical bits. For example, 0° and 45°polarization represents the binary bit 0, 90°, 135° corresponds to bit 1.
2. Quantum state preparation and transmission – Alice prepares single photon pulses and modulates their states of polarization to one of the four states according to the random bits stream she generated, then the pulses are sent to the quantum channel.
3. Detection – Bob measures the polarization of photons with random selected bases.
4. Sifting – Bob discloses the bases he used, then Alice tells Bob the bit slots in which she used the same modulation bases. They convert these detection results into binary bits according to the information agreement rules, thus the sifted key stream is generated.

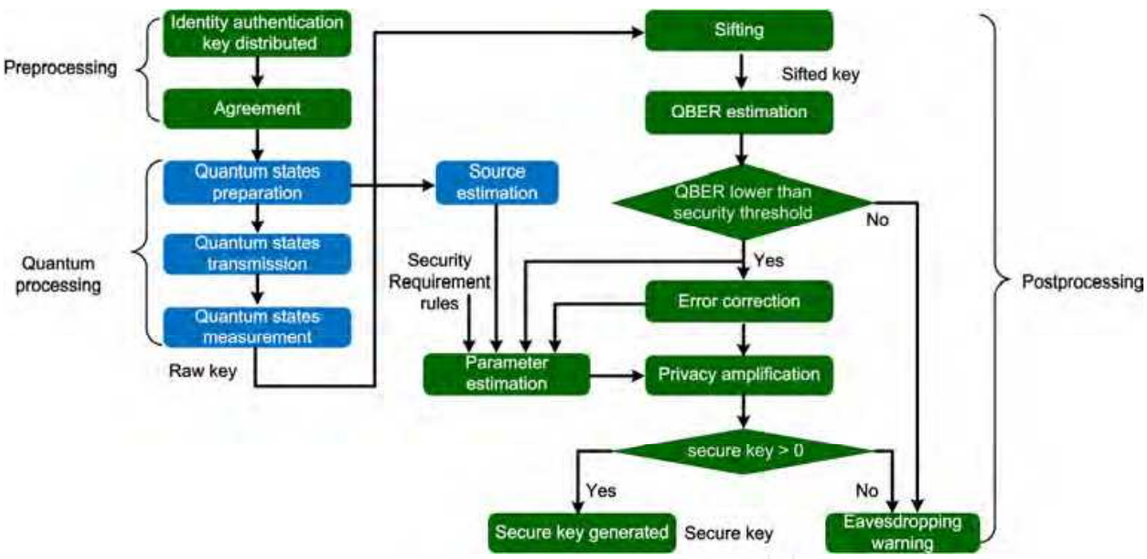



Fig. 1. Integrated QKD procedure

To generate a practice usable key stream in which Alice and Bob share uniform random bits while Eve has no secret key information, there are still some classical post processing works must be fulfilled, such as error correction and privacy amplification. The complete QKD session is shown in Fig. 1. From the diagram, we can see the security of QKD is not only depend on quantum processes, but also classical processes such as error correction, identification and authentication. The QKD without secure preprocessing and post-processing is not really secure. The first key stream used for authentication leads to a chicken-and-egg problem, which means QKD is essentially a kind of key expansion technology.

## 2. Security of quantum key distribution

The QKD protocol contains the quantum part and the classical part. In the quantum part, quantum states are prepared, transmitted and detected. Assuming that the noisy quantum channel can be controlled by the eavesdropper, the security of quantum channel can be proved by using the basic quantum mechanics property. A classical channel is necessary to apply the sifting, parameter estimation, error correction and privacy amplification to generate the final secure key stream. The classical channel should be authenticated with the unconditional secure authentication protocol based on 2-universal hash functions. The unconditional security analysis of protocols and systems has attracted a lot of attentions since the concept of QKD was proposed.

### 2.1 Security definition of QKD

Theoretical physicists have analyzed unconditional security of QKD in many respects. Initially, Lo and Chau (Lo, & Chau, 1999) proposed the security analysis with the help of quantum computer. Then, Shor and Preskill (Shor,& Preskill, 2000) proved that the security of prepare-and-measure protocol is equivalent to entanglement-based protocol, thus unconditional security of QKD has been proved combining with the CSS code and entanglement distillation and purification (EDP) technology. Without applying the EDP technology, the security of QKD with information theory method has been analyzed (Renner, 2008). More recently, the security of QKD based on private-entanglement states has been analyzed (Horodecki, 2008). Inspired by Horodecki's mind, Renes and Smith (Renes, & Smith, 2007) have analyzed noisy processing which allows some phase errors to be left uncorrected without compromising unconditional security of the key.

Security proof of perfect QKD protocol can be divided into three levels: physical explanation, physical proof and quantum information theory proof. Physical explanation is based on the no-cloning theorem and the uncertainty principle. Since the quantum state is encoded with two non-orthogonal bases, the eavesdropper Eve can not get the full secret information without disturbing the quantum state. More precisely, the uncertainty relation gives upper bounds on the accuracy by which the outcomes of two incompatible measurements can be predicated, the generalized uncertainty principle (Berta, et al., 2010; Tomamichel, & Renner, 2011) can be given as

$$H_{\min}^{\varepsilon}\left(X|B\right)+H_{\max}^{\varepsilon}\left(Z|E\right)\geq q \tag{1}$$

where $X$ and $Z$ are measurement outcomes with Pauli matrix $X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ and $Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$, the min-entropy $H_{\min}^{\varepsilon}\left(X|B\right)$ illustrates Bob's uncertainty about the measurement outcomes $X$, $q$ quantifies the incompatibility of the two measurements in Bob's side and Eve's side respectively. The max-entropy $H_{\max}^{\varepsilon}\left(Z|E\right)$ illustrates Eve's uncertainty about the measurement outcomes $Z$. From this equation, we find that the upper bound of Eve's information can be estimated by considering Bob's measurement outcomes. In case of BB84 protocol, we can apply the uncertain principle and estimate upper bound of Eve's information as the following

$$H_{\max}^{\varepsilon}\left(Z|C\right)\geq 1-H_{\min}^{\varepsilon}\left(X|B\right)=1-h\left(\delta\right) \tag{2}$$

where $h$ is the binary entropy function, $\delta$ is the quantum bit error rate. Physical proof is based on the entanglement based QKD protocol. Since the entanglement quantum state has the monogamy principle, Eve can not get the secret key in case of that Alice and Bob can establish the maximal entangled quantum state $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The monogamy correlation (Scarani, & Gisin, 2001; Pawlowski, & Brukner, 2009) can be given by

$$G^2_{CHSH}(A,B) + G^2_{CHSH}(A,E) \le 8 \tag{3}$$

where $G^2_{CHSH}(A,B)$ ($G^2_{CHSH}(A,E)$) is the Clauser-Horne-Shimony-Holt (Clauser, et al., 1969)(CHSH) inequality between Alice and Bob (Eve). Information theory proof (Renner, et al., 2005) is the most universal security proof, which illustrates the trace distance between the practical quantum state and the uniformly distributed perfect quantum state

$$\frac{1}{2}\left\|\rho_{practical} - \rho_{perfect}\right\| \le \varepsilon \tag{4}$$

where $\|M\| \equiv Tr\left\{\sqrt{M^+ M}\right\}$ is the trace normal of an Hermitian operator $M$, the perfect quantum state shared between Alice, Bob and Eve can be given by

$$\rho_{perfect} = \sum_{s\in S} |s\rangle\langle s|_{Alice} \otimes |s\rangle\langle s|_{Bob} \otimes \rho_{Eve} \tag{5}$$

$s$ is the secret key shared between Alice and Bob, $\rho_{Eve}$ is Eve's quantum state. Since Eve's quantum state has no correlation with Alice and Bob's quantum state, Eve can get no secret key. In case of the trace distance between the practical quantum state and the perfect quantum state is lower than $\varepsilon$, the practical quantum state has the same property comparing with the perfect quantum state with probability at least $1 - \varepsilon$.

### 2.2 Security of perfect quantum key distribution protocol

Suppose that Alice and Bob choose the polarization encoding QKD system in our security analysis, the standard prepare-and-measure QKD protocol will be introduced in the following section (Li, et al., 2011). In Alice's side, the classical bit 0 is randomly encoded by quantum states $|0^o\rangle$ or $|45^o\rangle$, the classical bit 1 is randomly encoded by quantum states $|90^o\rangle$ or $|135^o\rangle$. In Bob's side, he randomly choose rectilinear basis $\{|0^o\rangle, |90^o\rangle\}$ or diagonal basis $\{|45^o\rangle, -|135^o\rangle\}$ to measure the quantum state transmitted through the quantum channel. After Bob's perfect measurement and some classical steps of QKD (sifting, parameter estimation, error correction and privacy amplification), secret key bits can be shared between Alice and Bob. Following the technique obtained by Shor and Preskill, the security of prepare-and-measure QKD protocol is equal to the security of entanglement-based QKD protocol, which can be constructed by considering the corresponding prepare-and-measure encoding scheme as shown in Fig. 2 .

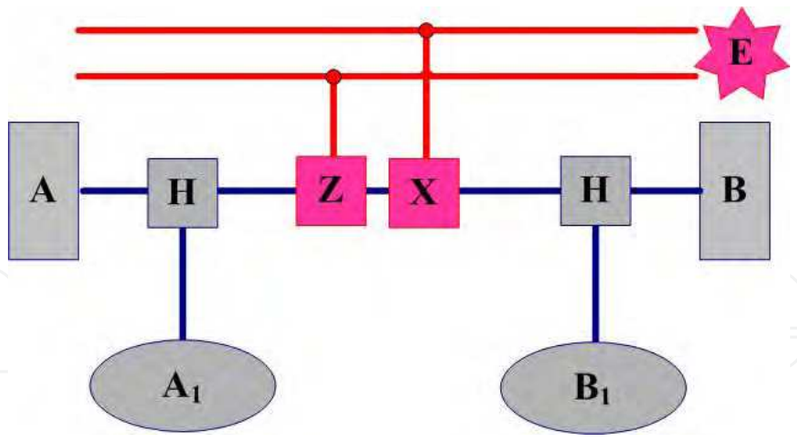



Fig. 2. Entanglement-based protocol with Pauli channel and eavesdropper Eve

Alice prepares maximally entangled pairs $|\phi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$. After applying the Hadamard operation randomly to the second part of the pair, she sends Bob half of the pair. Bob acknowledges the reception of his state and applies the Hadamard operation randomly. In the security analysis, the most generally noisy channels we need to consider are Pauli channels. By considering Eve's eavesdropping in the Pauli channel, the quantum state about Alice, Bob and Eve is given by

$$\sum_{u,v,i,j} \sqrt{P_{uv}Q_{ij}}\left(I_A \otimes H^i_{B_1} \mathrm{X}^u_{E_1} Z^v_{E_2} H^j_{A_1} |\phi\rangle |u\rangle_{E_1} |v\rangle_{E_2} |i\rangle_{B_1} |j\rangle_{B_1}\right) \tag{6}$$

where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the perfect Hadamard operator, which means the transformation between different bases. Note that the Pauli quantum channel can only introduce bit error ( X ), phase error ( Z ) and bit phase error ( Y ) respectively. $P_{uv}$ $u,v \in \{0,1\}$ means the probability of the operator $\mathrm{X}^u_{E_1} Z^v_{E_2}$ introduced by Eve, which should be normalized by $\sum_{u,v,i,j} P_{uv} = 1$. $Q_{ij}$ $i,j \in \{0,1\}$ means the probability of $H^i_{B_1} H^j_{A_1}$ matrix introduced by Alice and Bob respectively, which satisfies $Q_{ij} = \frac{1}{4}$ for Alice and Bob's random choice. After the sifting step, the case of $i = j$ will be discarded. We trace out $A_1$, $B_1$ and Eve's systems to get the following equation

$$\rho_{AB} = \sum_{u,v} P_{uv} \begin{pmatrix} \frac{1}{2} I_A \otimes \mathrm{X}^u_{E_1} Z^v_{E_2} |\phi\rangle\langle\phi| Z^v_{E_2} \mathrm{X}^u_{E_1} \otimes I_A + \\ + \frac{1}{2} I_A \otimes H_{B_1} \mathrm{X}^u_{E_1} Z^v_{E_2} H_{A_1} |\phi\rangle\langle\phi| H_{A_1} Z^v_{E_2} \mathrm{X}^u_{E_1} H_{B_1} \otimes I_A \end{pmatrix} \tag{7}$$

After transmitting through the quantum channel, the initially shared maximally entangled state can be transformed into Bell states using equation (8).

$$
\begin{aligned}
|\phi\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right) \\
|\phi\rangle_{bit} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right) \\
|\phi\rangle_{phase} &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} - |11\rangle_{AB}\right) \\
|\phi\rangle_{bitphase} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right)
\end{aligned} \tag{8}
$$

If the maximally entangled pairs $|\phi\rangle$ is transformed into Bell state $|\phi\rangle$, no error will be introduced in the quantum channel. However, if the maximally entangled pairs $|\phi\rangle$ is transformed into Bell states $|\phi\rangle_{bit}$ , $|\phi\rangle_{phase}$ and $|\phi\rangle_{bitphase}$ respectively, the bit error, phase error and bitphase error will be introduced by Eve correspondingly. Thus, the bit error rate and phase error rate can be given by

$$
\begin{aligned}
e_{bit} &= {}_{bit}\langle\phi|\rho_{AB}|\phi\rangle_{bit} + {}_{bitphase}\langle\phi|\rho_{AB}|\phi\rangle_{bitphase} \\
e_{phase} &= {}_{phase}\langle\phi|\rho_{AB}|\phi\rangle_{phase} + {}_{bitphase}\langle\phi|\rho_{AB}|\phi\rangle_{bitphase}
\end{aligned} \tag{9}
$$

Comparing with the previous two equations, we can get the difference between bit error rate and phase error rate is $e_{bit} - e_{phase} = 0$ . Thus, the phase error can be accurately estimated by the bit error rate in the perfect device case. Thus, the final secret key rate can be given by

$$
R = 1 - h\left(e_{bit}\right) - \mathrm{h}\left(e_{phase}\right) = 1 - 2h\left(e_{bit}\right) \tag{10}
$$

### 2.3 Security of practical quantum key distribution system

Whereas, security analysis model based on the perfect QKD protocol can not be directly applied to the practical QKD system. Gottesman, Lo, Lukenhaus and Preskill (Gottesman, et al., 2004) analyzed unconditional security of the practical QKD system and gave the famous secret key rate formula GLLP, combining their security analysis result with decoy state method (Hwang, 2003; Lo, et al., 2005, Wang, 2005) , which makes practical QKD system can be realized with weak coherent light source. But their security analysis can not be applied to the practical QKD system with arbitrary imperfections, which will introduce side channel attacks. Xu et al (Xu, et al., 2010) have experimentally demonstrated the imperfect phase modulator will introduce phase-remapping attack. Lydersen et al (Lydersen, et al., 2010) have proposed detector blinding attack with imperfect single photon detector (SPD), they demonstrated that imperfect SPD can be fully remote-controlled by utilizing specially tailored bright illumination. More recently, Weier et al. (Weier, et al., 2011) have proposed dead time attack with imperfect SPD, in which the eavesdropper can exploit the dead time effect of the imperfect SPD to gain almost full secret information without being detected. Thus, practical QKD device imperfections can lead to various types of attacks, which can't be covered by the unconditional security analysis based on the perfect QKD protocol. Major imperfections and attacking methods are summarized in Fig. 3.

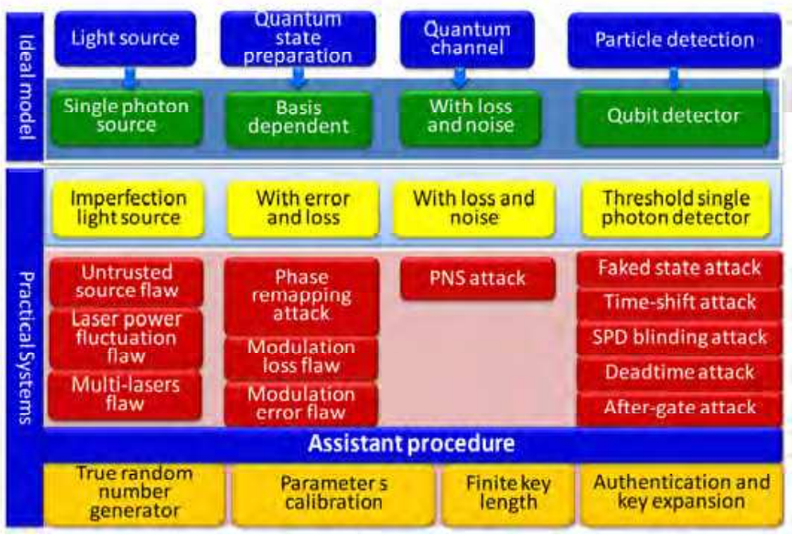



Fig. 3. The imperfections of practical QKD system and quantum hacking methods

Obviously, if the imperfection is basis-dependent, we can consider a slightly changed protocol, where the state preparation and measurement are perfect, while there is a virtual unitary transformation controlled by Eve introduces the basis-dependent imperfection in the quantum channel. Since security of the original protocol is no less than the slightly changed protocol, the final secret key rate can be estimated utilizing the GLLP formula. However, most of the imperfection in states preparation and measurement are state-dependent, which cannot be controlled by Eve in the security analysis. For instance, the wave plate may be inaccurate in polarization based QKD system, while the phase modulator may be modulated by inaccurate voltage in phase-coding QKD system. If the imperfection cannot be illustrated as an unitary transformation, it can't be considered as part of the quantum channel controlled by Eve.

### 2.3.1 Modulation loss of phase encoding QKD system

Most of real-life QKD implementations are based on phase-coding BB84 protocol, where Unbalanced Mach-Zehnder Interferometer (UMZI) (Gobby, et al., 2004) method is commonly used. However, the Phase Modulator (PM) in the interferometer is always imperfect, where the arm has the imperfect PM will introduce much more loss than the arm has no PM. In this case, photon state emitted by Alice's side is imperfect BB84 states, which we call it unbalanced states in the following.

$$\begin{aligned}
&\frac{1}{\sqrt{\mu+\nu}}\left(\sqrt{\mu}|1\rangle_s+\sqrt{\nu}|1\rangle_l\right)\\
&\frac{1}{\sqrt{\mu+\nu}}\left(\sqrt{\mu}|1\rangle_s+i\sqrt{\nu}|1\rangle_l\right)\\
&\frac{1}{\sqrt{\mu+\nu}}\left(\sqrt{\mu}|1\rangle_s-\sqrt{\nu}|1\rangle_l\right)\\
&\frac{1}{\sqrt{\mu+\nu}}\left(\sqrt{\mu}|1\rangle_s-i\sqrt{\nu}|1\rangle_l\right)
\end{aligned} \tag{11}$$

where, $|1\rangle_s$ is the quantum state in the short arm, $|1\rangle_l$ is the quantum in the long arm after the PM. In this equation, the mean photon number of the short arm $\mu$ is larger than the mean photon number in the long arm $\nu$ by considering the practical imperfect phase modulator. Correspondingly, secret key rate of QKD based on this states can not be estimated with GLLP formula directly. To give an optimal security key rate of QKD with unbalanced BB84 states, we propose that the real-life source can be replaced by a virtual source without lowering security (Li, et al., 2010).

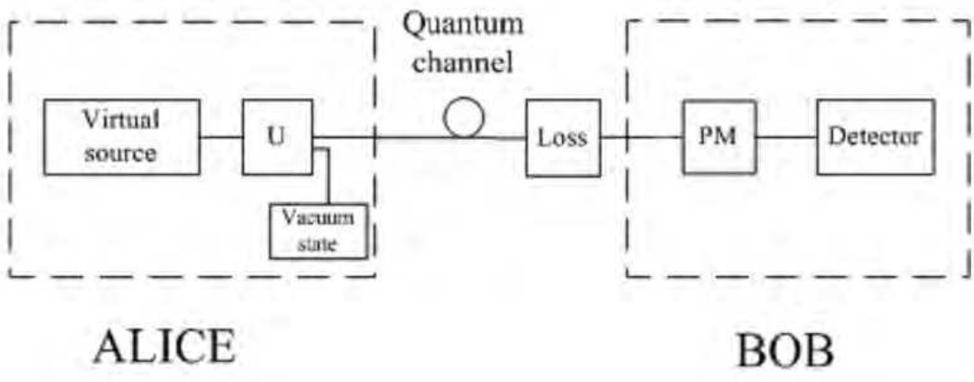



Fig. 4. UMZI method QKD with an imaginary unitary transformation and virtual source.

The unitary transformation does not need to be implemented in practical QKD experimental realizations, the detailed illustration of the unitary transformation is given as the following.

$$\begin{aligned}
&U|0\rangle_l|0\rangle_s|0\rangle_A = |0\rangle_l|0\rangle_s|0\rangle_A \\
&U|0\rangle_l|1\rangle_s|0\rangle_A = |0\rangle_l|1\rangle_s|0\rangle_A \\
&U|1\rangle_l|0\rangle_s|0\rangle_A = \frac{\sqrt{\nu}}{\sqrt{\mu}}|1\rangle_l|0\rangle_s|0\rangle_A + \frac{\sqrt{\mu-\nu}}{\sqrt{\mu}}|0\rangle_l|0\rangle_s|1\rangle_A \\
&U|n\rangle_l|m\rangle_s|0\rangle_A = |n\rangle_l|m\rangle_s|0\rangle_A \qquad n+m \geq 2
\end{aligned} \tag{12}$$

where, $|0\rangle_A$ and $|1\rangle_A$ are mutually orthogonal states. We can simply test and verify that the real-life setup of Alice can be replaced by the virtual source combining with the basis-independent unitary transformation. Obviously, we can even assume the unitary transformation is controlled by Eve, then the security of practical QKD setup is no less than the security of QKD with the virtual source.

### 2.3.2 Imperfect state preparation and measurement

We apply the entanglement distillation and purification (EDP) technology by considering the most general imperfect state modulation, and a much better secret key rate under constant imperfect parameters has been analyzed in comparation with previous works (Li, et al., 2011). The states prepared by Alice and measured by Bob both have individual imperfections as in Fig. 5, and the whole security analysis can be divided into two steps based on an virtual protocol as in Fig. 6.

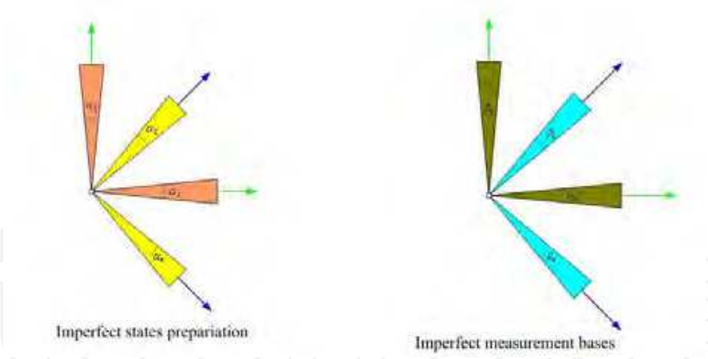



Fig. 5. The most general imperfect states preparation and measurement in practical QKD experimental realization.

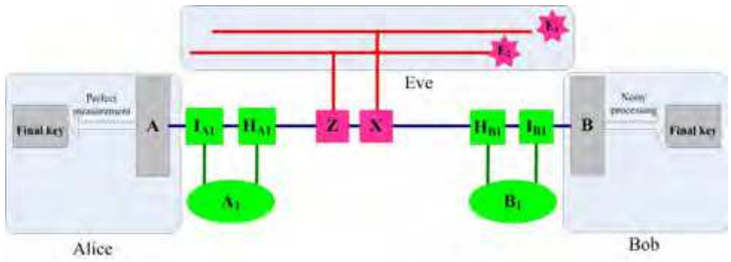



Fig. 6. Entanglement-based quantum key distribution protocol with imperfect devices.

Firstly, we consider that Alice prepares perfect entangled quantum state pairs, then she keeps half of the perfect entangled quantum state and sends half of the imperfect modulated quantum state to Bob, which illustrates the imperfect states preparation. Meanwhile, Bob applies perfect Hadamard transformation in the receiver's side, thus Alice and Bob can share the maximally entangled quantum state utilizing the EDP technology. Secondly, Alice applies perfect measurement with her maximally entangled quantum states, and Bob applies imperfect measurement with his entangled quantum states correspondingly, finally they can establish the raw key. Since the phase error introduced by Bob's imperfect measurement should not be controlled by Eve, we can get a much higher secret key rate correspondingly. The similar result has also been proved that adding noise in the classical post processing can improve the secret key rate by considering that the phase errors introduced in the post processing can not be controlled by Eve (Renner, et al., 2005). Comparing with the above security analysis result, the noise introduced by the imperfect device is precisely known by Eve, while the imperfection can not be corrected or controlled by Eve due to the random encoding choice. Thus, the exactly known but can't be controlled imperfection is similar to adding noise model (Kraus et al., 2005).

## 3. Realization of quantum key distribution – From point-to-point to network

The QKD system based on weak coherent pulses (WCP) is the most mature QKD technology up to date. The coherent laser pulse is attenuated to the single photon level, where photons are not equally distributed over the pulse train. The average photon number of 0.1 is an accepted secure threshold before decoy state is prompted. The most advantage of WCP QKD system is that the conventional diode lasers and standard single-mode optical fibers of 1550nm can be used, so that the transmission length can get maximum and the system can

be realized and integrated into the current fiber network at reasonable price. Here we focus on phase encoding WCP QKD system and fiber QKD network. Security, stability, integration and cost are major aspects of a practical QKD system. We should setup QKD systems with available light sources, encoder, decoder and detector. The flaw between theoretical model and practical devices must be filled by technical skills at acceptable cost .

### 3.1 Faraday-Michelson QKD system

A typical fiber QKD scheme is based on fiber Mach–Zehnder (M-Z) interferometers, which are unstable due to the polarization fluctuation caused by environment associated fiber birefringence (Han, et al., 2004). The polarization controllers and polarization recovery sessions are necessary in M-Z system to keep the system continuously operating. We presented a Faraday-Michelson (F-M) QKD system which is intrinsic-stable in fiber channel (Mo, et al., 2005). The Faraday rotate mirror can change any imcoming polarization state into its orthogonal state. The system uses this effect to automatically compensate the polarization fluctuation of the fiber channel and the system optical units. The BB84 F-M QKD system with decoy states is implemented, as show in Fig. 7. The quantum and the sync light pulses are generated using different lasers. The energy of the quantum light pulses are attenuated to the single-photon level, then be randomly modulated by the intensity modulator to generate the decoy-state pulses. Alice applies driving signals to her phase modulator to randomly encode binary information onto the photons, with phases of 0, $\pi/2$, $\pi$ and $3\pi/2$. The receiver Bob also randomly modulates the four phases of his phase modulator, then the interference results are delivered into an InGaAs/InP avalanche single photon detector (SPD). According to the BB84 protocol, the bases are divided into two sets consisting of $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$, in which phases 0 and $\pi/2$ denote bit 0, while $\pi$ and $3\pi/2$ denote bit 1. The users declare the basis sets they selected in every time bin in which the receiver detected photons, and the sifted keys with the same basis sets are kept.

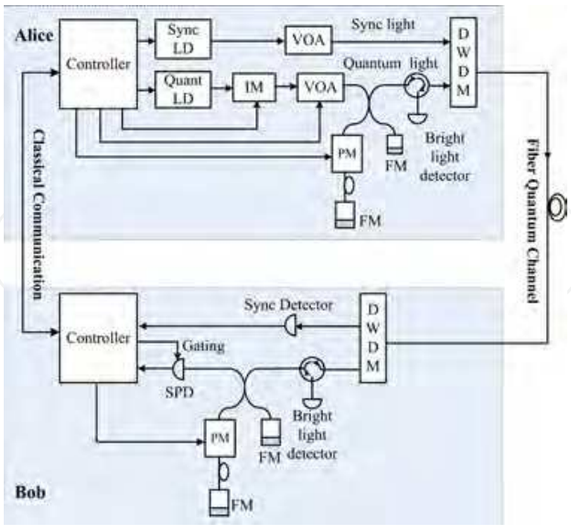



Fig. 7. The schematic diagram of Faraday-Michelson QKD system. Sync LD: Synchronization laser diode; Quant LD: Quantum laser diode; IM: intensity modulator; VOA: Variable optical attenuator; PM: Phase modulator; FM: Faraday rotator mirror; DWDM: Dense wavelength division multiplexer; SPD: Single photon detector.

### 3.1.1 Implementation essentials of secure QKD system

#### 3.1.1.1 The decoy states

The quantum light source used in the system is the weak coherent pulse laser which follows Poisson distribution and has a chance to prepare multi-photo pulses. The multi-photon part of the quantum signal is vulnerable to photon-number splitting (PNS) attack. Decoy state is proposed to resist the PNS attack by randomly modulating the average photon number of quantum signal. The kernel of decoy method is to estimate the lower bound of the secret key generated by the single photon state. More precisely, applying the formula of key generation rate (GLLP) with practical source as the following

$$r \geq \frac{1}{2}\left[Y_1 P_1\left(1-h\left(e_1\right)\right)-Q_\mu h\left(E_\mu\right)\right] \tag{13}$$

where, $r$ is the final secret key rate, $1/2$ is the sifting efficiency, $Y_1$ is the yield of the single photon state, $P_1$ is the proportion of the single photon state, $e_1$ is the quantum bit error rate (QBER) of the single photon state, $Q_\mu$ is the gain of the signal photon states, $E_\mu$ is the QBER of the signal photon states, $h$ is the binary Shannon information function. From the secret key rate formula, the upper bound of $e_1$ and the lower bound of $Y_1$ can be estimated. In practical side, suppose Alice and Bob choose decoy states with expected photon number $\nu$, then $Y_1$ and $e_1$ can be given by

$$\begin{aligned} Y_1 &\geq \frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - Q_\mu E_\mu e^\mu \frac{\mu^2-\nu^2}{\frac{1}{2}\mu^2}\right) \\ e_1 &\leq \frac{Q_\mu E_\mu}{Y_1 \mu e^{-\mu}} \end{aligned} \tag{14}$$

Combining this inequations with GLLP formula, the final secret key rate can be analyzed with the decoy state method. Note that the security of decoy state QKD protocol is based on that eavesdropper can not distinguish the signal state and decoy state with the same photon number.

The modulation speed of IM is same as the quantum signal generation rate, and the average photon number is randomly modulated to 0.6 and 0.2, which is used for signal and decoy states respectively. To generate the vacuum state, the quant laser will not be triggered. The ratio of the signal pulse, decoy pulse and vacuum pulse is 6:3:1 in the system.

#### 3.1.1.2 The single SPD scheme

In regular BB84 system, two single photon detectors are necessary, which correspond to bit 0 and bit 1 individually, and Bob only perform two-basis modulation. Due to the quantum efficiency mismatch of the multi-SPDs, these schemes are vulnerable to practical attack like fake-state attack and time-shift attack. In our system, the standard BB84 modulation pattern is modified. We use only a single SPD with the four-state modulation in Bob's side. This scheme has advantages to resist these kinds of attacks, but loses half of the detection events.

#### 3.1.1.3 For trojan attack

There are two optical circulators in the system. The optical circulators are used to make the system to immunize from Trojan attack, in which Eve would inject a bright light to the system and get information from reflected light. The optical circulator can restrain the light path as follows: the light incomes from port 1 will exits from port2, and the light from port2 will emit to port 3, as shown in Fig. 8. The bright light detectors of Alice and Bob are used to detect Trojan attack.

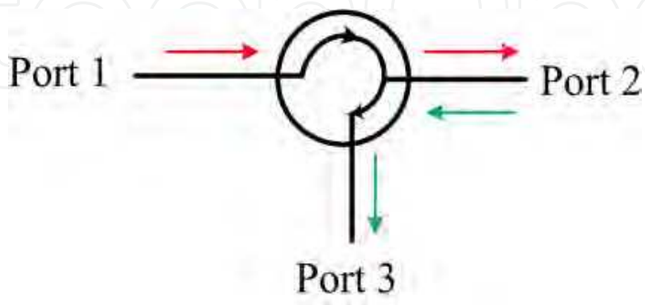



Fig. 8. The light path of optical circulator

#### 3.1.1.4 For bright illumination attack

The bright light detector in Bob's side is not only for detecting Trojan attack, but also for detecting bright illumination attack. The bright light emits into detection system will be reflected by the Faraday rotator mirror and split by a fiber optical coupler, the reflection light will be guided by optical circulator and reaches the bright light detector. The total loss of the bright illumination light is about 3.5~4.5 dB. Since the light power used to effectively blind the SPD is regularly in the level of μW~mW, it can be detected by conventional bright light detectors.

### 3.1.2 The measures to keep system stable

#### 3.1.2.1 Self-compensation of birefringence

Since the perfect interference requires exactly the same photon polarization, the birefringence also has influence to the phase encoding system. The unbalanced Michelson interferometer combined with Faraday rotator mirror can effectively compensate the birefringence of the fiber devices and channel. The Faraday rotator mirror is designed to rotate a signal's state of polarization (SOP) by 90°. Once 45° when the light enters, and again when the light is reflected back. Since the Faraday effect is non-reciprocal, the resultant SOP is rotated by 90° with respect to the original signal. The birefringence of the fiber channel can be self-compensated thanks to this character of Faraday rotator mirror (Mo, et al., 2005).

#### 3.1.2.2 Synchronization

The SPD used in the system is based on InGaAs/InP avalanche photodiode (APD), which can respond to a single photon. This kind of APD needs to operate in Geiger mode to achieve single photon sensitivity with a low dark count rate. The gating signals of narrow pulses should be added to the bias when the photons arrive, so that sync signals for gating are necessary. Typically, there are two means to transfer synchronization light pulse - to use

a standalone fiber or combine the sync single into the quantum channel. Although the crosstalk from sync light is minimum in the former scheme, the time base drift caused by the environment and the length difference between two fibers must be well compensated. The timing drift of the latter scheme is much smaller, but the crosstalk should be effectively reduced. Here we chose the one-fiber scheme not only for gating time stabilization but also to save the fiber sources. In order to suppress the interference from sync light, conventional avalanche photodiodes with typical sensitivites of -35dbm are used as sync detectors, which denotes the power of the sync light can be attenuated much.

#### 3.1.2.3 Phase drift compensation

The phase drift is a common problem in phase encoding QKD system, and must be solved for long time operating QKD sessions, as shown in Fig. 9 (Chen, et al., 2008). Generally, there are three methods to solve the problem: Modify the structure of interferometers such as ”plug-and-play” configuration to auto-compensate the phase shift. Use passive compensation to reduce the negative effect of environment fluctuations by strict thermal and mechanical isolation. Acquire drift parameters by active phase tracking then perform compensation. Here, we proposed a four-phase scanning software compensation method without adding additional reference light or hardware feedback unit (Zhang, et al., 2010). The software method is more suitable for high speed QKD system, because the reference light for compenstation maybe cause severe crosstalk to quantum signal in this senerio. The four-phase scanning method bases on the interference fringe and the coding matrix. The interference fringe is the curve of the relationship between the SPD counts and the phase difference between Alice's and Bob's phase modulator. Either site, for example Alice, fixes its phase modulation voltage as $V_{ref}$ which denotes the corresponding phase shift as $\varphi_{ref}$. The opposite site, i.e. Bob scans its phase modulation voltage from 0 to the full scale range of the DAC (its output voltage controls the phase shift) in a number of steps. In our setup, the phase modulation voltage ranging from -6V to 6V corresponds the phase shift ranging from 0 rad to more than $2\pi$ rad. Therefore, scanning the control voltage will traverse 0 to $2\pi$ phase differences, as shown in Fig. 10.

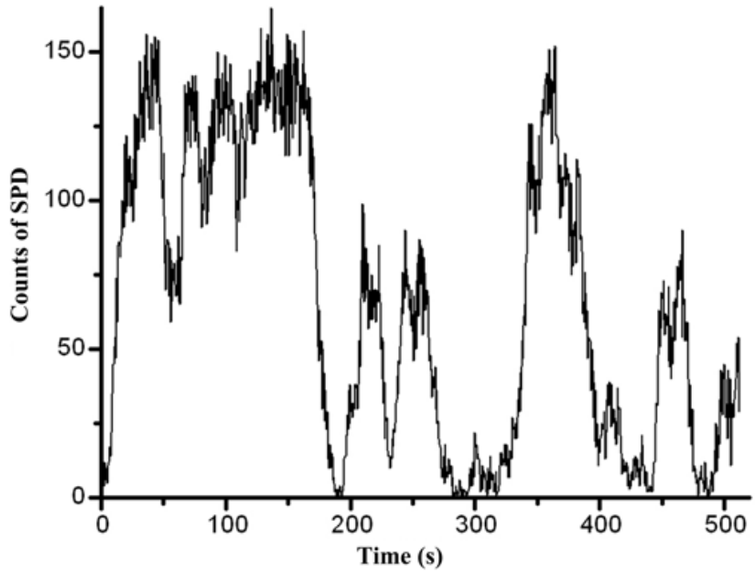



Fig. 9. Phase drift in a QKD experiment

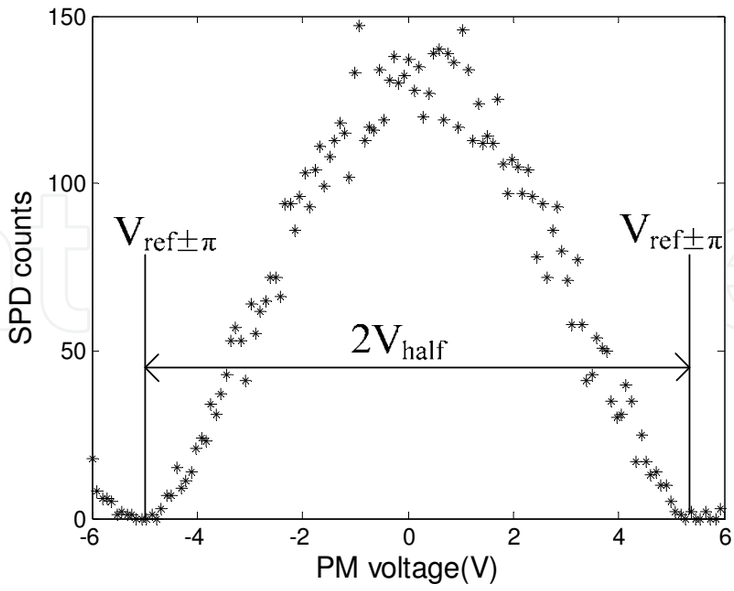



Fig. 10. Interference fringe

At each scanning step, Alice transmits a certain number of photons, meanwhile Bob records the number of photons detected by SPD, so we can get the curve of counting intensity versus the phase difference. The process fixing A-side at $V_{a,\ ref}$ and traversing B-side is called scanning B (relative to $V_{a,\ ref}$). Through the interference fringe from the scanning B, we could get two important parameters on B-side modulator. One is the half-wave voltage (denoted by $V_{b,\ half}$), which is the voltage difference of the half cycle of the interference fringe. The second parameter is the destructive interference voltage, which is the voltage at the valley of the interference fringe, and is denoted as $V_{b,\ ref\pm\pi}$. The phase difference between voltages $V_{a,\ ref}$ and $V_{b,\ ref\pm\pi}$ is $\pi$. By the process scanning A, we can get these two parameters for A-side modulator, they are $V_{a,\ half}$ and $V_{a,\ ref\pm\pi}$. The flow of algorithm is described below:

**Step 1.** Alice gets the half-wave voltage ($V_{a,half}$) by scanning her interference fringe. Assuming its zero phase modulation voltage is $V_{a,0}$, Alice can estimate her voltages for the four phase shifts ($V_{a,0}$, $V_{a,\pi/2}$, $V_{a,\pi}$, $V_{a,3\pi/2}$) as ($V_{a,0}$,$V_{a,0}$+1/2$V_{a,half}$, $V_{a,0}$+$V_{a,half}$, $V_{a,0}$+3/2$V_{a,half}$), respectively.

**Step 2.** Setting Alice's phase modulation voltage $V_{Alice,ref}$ as 0, $\pi/2$, $\pi$, $3\pi/2$ in turn, Bob scans his interference fringes. From these four interference fringes, Bob obtains his destructive interference voltages as ($V_{b,0\pm\pi}$, $V_{b,\pi/2\pm\pi}$, $V_{b,\pi\pm\pi}$, $V_{b,3\pi/2\pm\pi}$). These are exactly equal to Bob's four phase modulating voltages ($V_{b,\pi}$, $V_{b,3\pi/2}$, $V_{b,0}$, $V_{b,\pi/2}$).

**Step 3.** By checking the difference between the ideal coding matrix and the calculated coding matrix, Alice's four phase modulation voltages ($V_{a,0}$, $V_{a,\pi/2}$, $V_{a,\pi}$, $V_{a,3\pi/2}$) are tuned and step2 and step3 are repeated until the difference is sufficiently small. Then the current voltages ($V_{a,0}$, $V_{a,\pi/2}$, $V_{a,\pi}$, $V_{a,3\pi/2}$) and their scanning results ($V_{b,\pi}$, $V_{b,3\pi/2}$, $V_{b,0}$, $V_{b,\pi/2}$) will be used in the normal transmission process. The diagram of the algorithm flow and the results of the experiment is shown in Fig. 11.

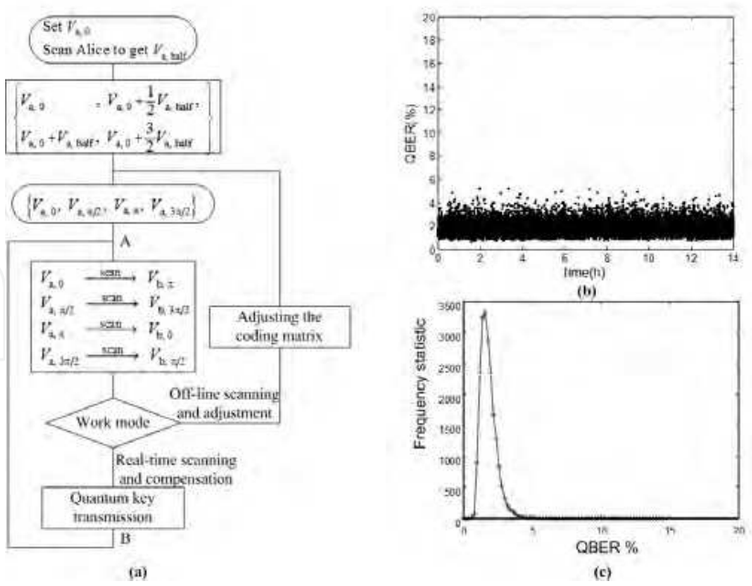



Fig. 11. Flow diagram of the four-phase scanning method and the experiment result. (a) Flow diagram, (b) QBER record of QKD experiment over 1 hours, (c) QBER statistic result.

The Faraday-Michelson (F-M) QKD system has been tested in 125Km dark fiber from Beijing to Tianjin in China in 2004. The QBER was less than 6%, which was mainly limited by the dark count of SPD. This scheme is used as the physical layer apparatus in our next QKD network experiments.

### 3.2 QKD network

A point-to-point system is not enough to satisfy network communication requirements in real life, so building a quantum key distribution network is not only necessary but also crucial to practical quantum cryptography. Unfortunately, the quantum mechanics make usual network routing methods invalid while keeping the QKD system secure. There are several difficulties to build QKD network.

1. The power of signal is limited at the single-photon level and can't be amplified, which indicates that it is possible but infeasible to get enough signal to noise ratio (SNR) by increasing the light power.
2. The signal can't be relayed in a classical measure and resend manner. Furthermore, it is hard to encode the light signal due to the fiber loss. It indicates the packet switching used in internet is no longer applicable.

The switch units in QKD network can be divided into three categories: optical unit, trusted relay, and quantum repeater. Among them, quantum repeater is still in the lab research stage and far away from real-life applications. Trusted relay requires the quantum signals to be converted into classical binary key bits, so that the quantum features of the keys are eliminated. The security controls of the sites where trusted relay located will become a serious problem while the network scale expands. For now, in existing QKD network, trusted relay is the most available approach to prolong the key distribution distance. Optical components can keep the quantum features of the particles, however the secure key

distribution distance can't be extended. So far several optical QKD network schemes have been presented. In the 1990s, A looped and branched network was firstly proposed (Townsend, et al., 1994), then QKD sessions between one controller and several terminals in a branched network were demonstrated, in which the kernel part is a beam splitter (Towsend, 1997). After that, several QKD local network topologies have been proposed with optical methods (Nishioka, et al., 2002; Kumavor , et al., 2006; Fernandez, et al., 2007; Ma, et al., 2007; Zhang, et al., 2008 ). In this chapter, we will focus on the metropolitan fiber QKD networks set up by optical components.

### 3.2.1 A QKD network scheme

Here we propose a star topology QKD network based on wavelength-division multiplexing (WDM) in which all users can exchange keys directly and simultaneously, which we call real-time full connectivity (RTFC) network. The center of the network is a "QKD router" (QR). For an N-user network, the QR has N ports and each user connects to one port of the QR via a fiber. A user transfers photons of different wavelengths to the QR and these photons are delivered to a certain user according to their wavelengths. For any two users who want to communicate with each other, a unique wavelength is assigned to them and this is regarded as an address code for the destination of the photons. This scheme provides unique optical links between each two pairs of transmitters and receivers, and arbitrary point-to-point fiber QKD systems can be used as physical equipments into the network. The only change for point-to-point system is that two multiplexers are added into the communication link. However, the maximum secure transmission distance will be reduced a little due to the additional insertion loss.

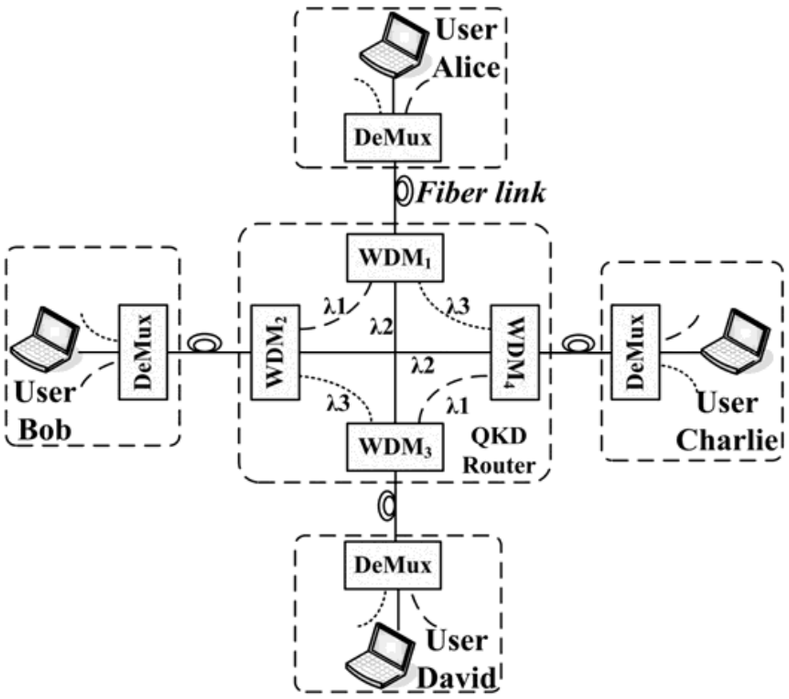



Fig. 12. Structure of four-user QKD router and the star network topology. DeMux: demultiplexer.

As an example, a four-user QKD network is used to describe the topology, as shown in Fig. 12. The router is composed of three-wavelength WDMs. When Alice wants to send quantum signal to Bob, she selects wavelength $\lambda_1$ corresponding to the specific connection inside the router, as shown in Fig. 12. These photons will be demultiplexed by $WDM_1$ and transmitted to $WDM_2$ through the link $\lambda_1$ between $WDM_1$ and $WDM_2$, then forwarded to Bob. Alice can transmit photons of $\lambda_1$, $\lambda_2$ and $\lambda_3$ at the same time in principle, then she can exchange keys with Bob, David and Charlie simultaneously, although the cost will increase. The operations of all other users are the same as for Alice. The network can be extended to N users, concurring with the edge coloring theorem in graph theory. Each WDM, link, and wavelength corresponds to a vertex, edge and color in the graph, respectively. From the edge coloring theorem, N-1 colors are required to render a complete graph with N vertices when N is even, and N colors when N is odd. This means that for an N-port router, each WDM should be an N-1 (when N is even) or N (when N is odd) wavelength multiplexer. As the network expanding, crosstalk will become the main constraint.

The crosstalk of the QKD network can be termed as interband (intraband) crosstalk, the wavelength of which falls outside (inside) the same wavelength band as the signal. The interband crosstalk can be removed by narrow-band filter (NBF) in principle. Using thin filmfilter 100GHz dense wavelength division multiplexing (DWDM) filter, less than -32dB (-48dB) adjacent (non-adjacent) channel crosstalk can be obtained experimentally. The maximum QBER caused by 40 interband crosstalk will be $0.5\times10^{-3.2}\times2+0.5\times10^{-4.8}\times38\approx0.10\%$, which validates that the interband crosstalk can be neglected in such a small size QKD network. The intraband crosstalk, which can be categorized into coherent and incoherent crosstalk, can't be eliminated by NBF and will cause non-ignorable QBER. Assuming the counting probabilities of signal and crosstalk photons are $a_s$ and $a_c$. The total photon counting probability of the coherent crosstalk should be $|a_s+a_c|=|a_s|^2+|a_c|^2+2Re[a_s a_c^*]$, while in the incoherent crosstalk, the third component is 0 in long time statistic. The intraband crosstalk in the network is mainly caused by the multi-path reflection of the quantum signal itself and the same wavelength photons from other users' lasers. The photons from different lasers are generally considered to be incoherent. Since the fiber length in the router is generally much longer than the coherence length of the laser, the mulit-path crosstalk from the same laser is also incoherent. Furthermore, the multi-path crosstalk here can be neglected while taking the return loss of WDM into account.

In QKD network, the average photon number of each user's quantum signal should be fixed and equal when they access into the fiber link, therefore the power penalty model is not suitable for evaluating QKD network. The crosstalk photons generate photon counting only when they fall into the "Geiger" mode SPD triggering gate, and there will be no bit error when the signal and crosstalk photons arrive simultaneously. Thus the maximum QBER is occurred when the crosstalk photons entirely unoverlap with the signal photons, and can be depicted as

$$QBER=\frac{1-V}{2}+\frac{p_{dark}+n_c q\mu\delta 10^{-0.1(\gamma+\alpha+\beta L_c)}\eta}{2(q\mu\delta 10^{-0.1(\gamma+\beta L_s)}\eta+p_{dark}+n_c q\mu\delta 10^{-0.1(\gamma+\alpha+\beta L_c)}\eta)} \tag{15}$$

where V is the fringe visibility of the optical system, which is around 98% in our system. $p_{dark}$ is the dark count rate of SPD, $q$ is the protocol efficiency which is 0.5 with BB84. $\mu$ is the average photon number of the signal and crosstalk accessing into the quantum channel. $\delta$ is the system-related loss, which is 1/2 in F-M system. γ is the insertion loss of the router (typically 2.5dB). $\beta$≈0.2dB/km is fiber loss factor. $\eta$ is the detector's quantum efficient, which is about 10% typically. $L_c$ and $L_s$ is the fiber length of crosstalk and signal link respectively. $n_c$ is the number of the crosstalk and $a$=32dB is the isolation of the router.

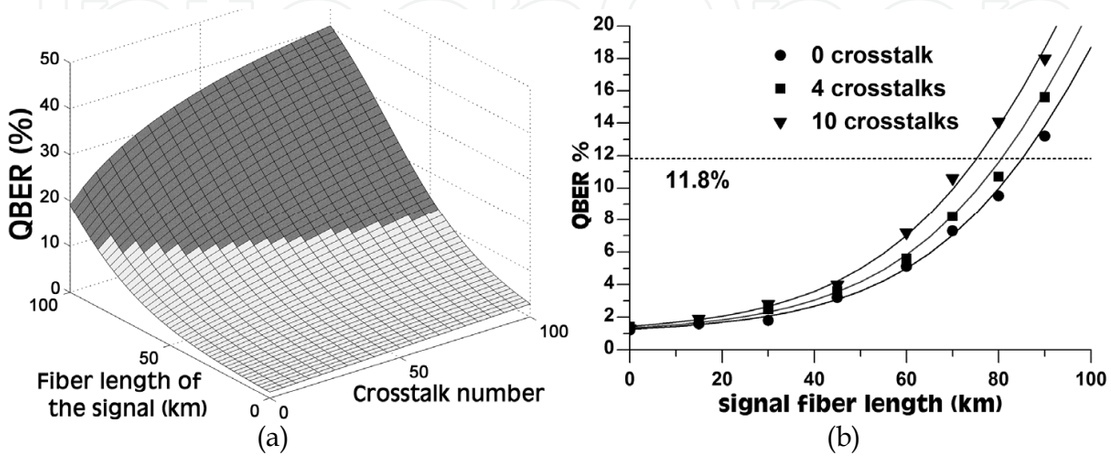



Fig. 13. (a) Simulation result of maximum QBER as a function of intraband crosstalk number and fiber distance, the QBER of the black filled area is more than secure threshold of 11.8%; (b) Experimental results of the maximum QBER of 0, 4 and 10 intraband crosstalk sources in the network, lines are the theoretical value and points are the experimental.

Since simplex transmission is enough to fulfill QKD, only (N-1)/2 or N/2 homodyne links will exist in an odd or even user number QKD network, respectively. Using the parameters in the field experiment and assuming $L_c$=0, in which the most critical situation is, the maximum QBER of the network is simulated and experimentally evaluated in lab, as shown in Fig. 13. The result indicates that it is possible to build a 200-user QKD network covering a 50km diameter metropolis with the basic QBER requirement. The QBER lower than 5% is generally required to effectively generate secure key if we take practical post processing of decoy into account, so that the valid user number will be a little reduced to 80-100.

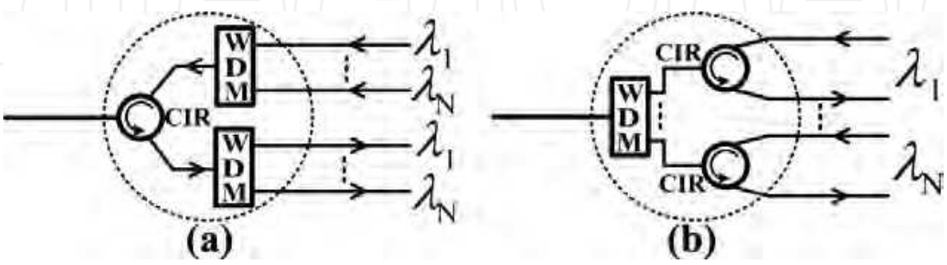



Fig. 14. Two structures of the basic unit. $\lambda_1 \ldots \lambda_N$ are N wavelengths band of WDM, and arrows mark directions.

Wavelength is a strained communication resource. We proposed a wavelength-saving RTFC QKD network scheme utilizing the simplex character of QKD (Wang, et al., 2010). The QKD

network with the new topology can support 2N + 1 nodes only with N wavelengths, which saves about 50% of the wavelengths compared with the previous topology. The wavelength-saving topology employs the basic unit consisting of one three-port circulator (CIR) and two N-wavelength WDMs as show in Fig. 14 (a)Fig. 13, or one N-wavelength WDM and N three-port CIRs Fig. 14 (b). This basic unit can be regarded as a multiplexer joining N input signals together and a demultiplexer splitting N output signals apart, denoted as M&D.

As an example, Fig. 15 shows the topology of a five-node RTFC QKD network with two wavelengths. Every node connects to the QKD router, which is composed of five 1 × 4 M&Ds. When node A wants to share secret keys with B, its QKD transmitter A2B sends photons of wavelength $\lambda_1$ to its M&D, which multiplexes these photons to the optical fiber channel; while arriving at the router, these photons will propagate from port 1 to 2, then forward to B and be demultiplexed by the M&D, and finally received by the corresponding B QKD receiver A2B. At the same time, node A wants to share other keys with D, which would be required to send photons of wavelength $\lambda_2$ to A. Therefore, A can transmit photons of wavelength $\lambda_1$ and $\lambda_2$ to B and C, and receive photons of wavelength $\lambda_2$ and $\lambda_1$ from D and E, respectively, simultaneously. Every node in this architecture is on the same term, so every two nodes can share secure keys directly at the same time only with two wavelengths. Because photons in the network propagate is unidirectional (only from one node to the other), any one-way P2P QKD system can be applied on this QKD network independently. According to the Hamiltonian circuits theorem in odd complete graph theory (Deo, 1974).

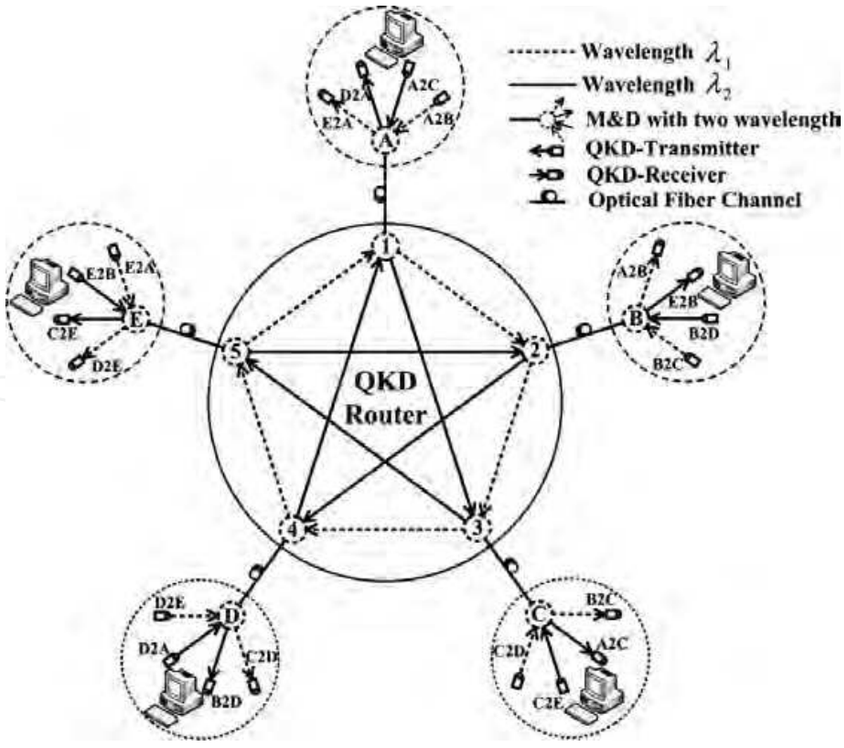



Fig. 15. Schematic diagram of the five-node QKD network topology with two wavelengths. A, B, C, D, and E are the five nodes, and 1, 2, 3, 4, and 5 are the five ports of the QKD router. Arrows indicate the propagation direction of the photons.

### 3.2.2 The QKD network in field

Some field QKD networks ,such as the DARPA (Elliott, et al., 2006), the SECOQC (Peev, et al., 2009) and the Tokyo QKD network (Sasaki et al, 2011) have been reported in the world. In China, the first field metropolitan QKD network with four users was implemented in the commercial backbone fiber network of China Netcom Company Ltd (CNC) in Beijing, 2007 (Chen, et al., 2009). The longest distance between two users is 42 Km and the shortest is 32 Km. The decoy state F-M QKD system was implemented in the network.

In 2009, A more complex QKD network was implemented in Wuhu, the five users nodes in which located in government bureaus (Xu, et al., 2009). The structure of the network is shown in Fig. 16(a). In this network, we constructed different priorities by considering the requirement of the bureaus. For four important nodes, a high-level full mesh backbone network was built among them and each of them can also operate as a trust relay to expand the net. Two of the others belonged to a subnet, linked with an optical switch matrix to one trust relay node shown as Node "D" in the diagram of the backbone network. In addition, we used one single telecom fiber to add the seventh node into the network, for both the classic network connection and QKD distribution, to infer the potential of our QKD network even if the fiber channel is limited. The whole quantum cryptographic network was built on the inner-city telecom fiber cables with the distribution in the satellite map of Fig. 16 (b). The network was totally implemented with decoy state QKD systems and the wave-length saving scheme was adopted.

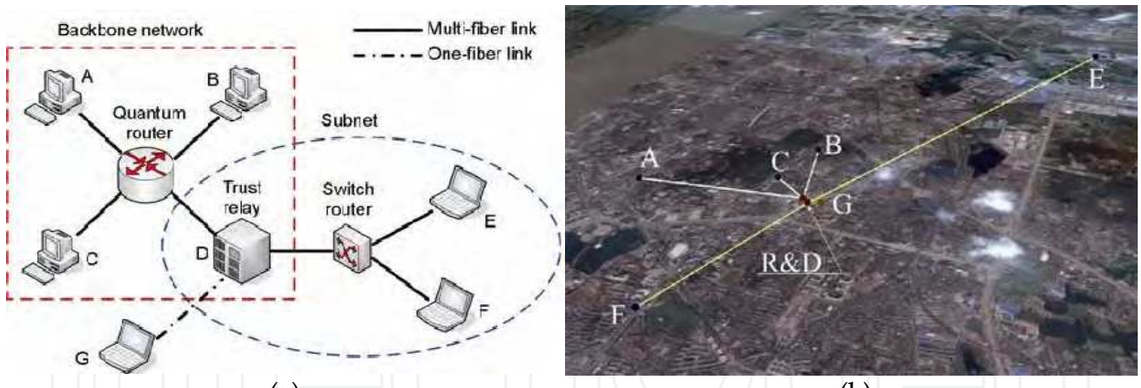



Fig. 16. (a) Structure of the hierarchical quantum cryptographic network, which contains techniques of QKD router, trust relay and switch router. A to G stand for seven different terminal nodes, which linked to the backbone in the red dash square and the subnet in the blue dash circle individually. (b) Distribution map of the nodes in the network. Node A located in the Bureau of Science and Technology. B stands for the building of Economic Committee. C was in the office of General Labour Union. R stands for the QKD router, which located in the same telecom station with Node D. The backbone network was composed of these four nodes. E and F belonged to the subnet, and was settled in the Bureau of Quality and Technical Supervision and the Civic Commerce Stimulus Bureau respectively. G was in the telecom station as well.

| | A2R2B | A2R2C | C2R2E | C2R2F |
|---|---|---|---|---|
| Wavelength (nm) | 1530 | 1550 | 1530 | 1550 |
| Attenuation (dB) | 7.24 | 8.78 | 14.77 | 10.79 |
| Sifted key (kbps) | 31.00 | 17.64 | 3.83 | 8.16 |
| QBER (%) | 2.92 | 2.84 | 3.76 | 2.78 |
| Secure key (kbps) | 4.91 | 2.02 | 0.41 | 1.82 |

Table 1. Field test results for QKD network

The clock of the system was 20MHz, and the test results are shown in Table 1. Using the secure key bits generated by QKD sessions, encrypted tele-meetings between the Bureaus in the network were demonstrated. With the quantum systems used in the network, the key generation rate was insufficient for one-time-pad encryption of high bit rate multimedia data stream, and so therefore, the advanced encryption standard (AES) algorithm with the 128-bit key stream updated every one minute was implemented. The low bit rate speech data in the link A2R2B, text messages and confidential files in all links were transmitted using a one-time-pad encryption.

## 4. Application of quantum cryptography

Here we would like to survey the quantum cryptography from the user's point of view. Maybe some of the viewpoints expressed here are not original nor objective. These perspectives only represent our understandings of quantum cryptography.

### 4.1 The application motivation

Undoubtedly, security is the top power to drive scientists, engineers to research quantum cryptography and the customers to keep a watchful eye on this technology. The problems asked by customers may be like if this quantum "unconditional security" can be really realized? and what benefits can this unconditional security bring? How much will it cost? and so on. The customers can be divided into three categories, the representative of which are academy, government, and business users. The academical customers is similar to the researchers, scientific research is their major motivation to adopt quantum cryptography, so that they are regarded as researchers rather than customers. This part of market is limited and no rapid growth can be anticipated. The requirements of the government are a little complex. The perfect secure communication is attractive for the government. On the other hand, they need to keep ability to monitor the communication in necessary occasions in order to keep national security. The contradiction is their original driving force to support quantum cryptography development. This kind of users are strictly care the real-life security rather than cost. The business customers such as group corporations also have remote secure data transfer requirements. There are some motivations to make customers update their technologies when the existing solutions have been adopted:

necessary upgrading functions, much cheaper payments, much more effective or convenient way. In the view of these users, the benefits and the cost must be seriously evaluated.

After more than 20 years of development, quantum cryptography has been understood by a lot of people. The gap between the theoretical description and the real-life realization of quantum cryptography is also well known. Especially, the quantum hacking experiments published in 2010 even lead to a crisis of confidence of quantum cryptography. Since it is well known that unconditional security equals to unconditional investment, making people aware of the weakness of quantum cryptography is not an aggravating situation, but the necessary step to make quantum cryptography technology mature. After that, the proper usage manners and conditions of quantum cryptography can be declared correctly.

From the vendors' and researchers' point of view, the investment of information safety is still not enough and the road of the commercial QKD is full of obstacles. Even if the acceptable security of quantum cryptography is guaranteed, its function is still limited. The information security generally includes storage security, transmission security, authentication security, perimeter security and management security. Quantum cryptography can't solve all these problems. Besides, conventional cryptographers are also developing new crypto technologies to resist future attacking, such as quantum computation, in a much cheaper price than QKD, so that the cost performance will be a critical factor for business users.

### 4.2 Technology maturity

The secure key generation rate, the maximum key distribution distance, the quantum channel requirements are main technical roadblocks in real-life QKD. At present, the light pulse repetition rate has reached 10GHz and the distance over 200Km, the secure key rate in 50Km fiber can be over 1Mbps, which can support OTP video encryption. The commercial communication for a single mode optical fiber bandwidth has reached 40Gbps and the systems aim at 400Gbps to 1Tbps are in developing. The key generation performance of QKD is far from that record, so that its applications are limited in low speed communication occasions when adopting OTP. Besides that, QKD is mainly restrained in metropolitan area due to its maximum transmission distance. The research achievements of quantum repeater and satellite QKD would help to overcome the defect, however, the trusted relay is still the only choice for now.

The requirement of quantum channel either in fiber or in free space is a serious problem, which is in contradiction with the tendency of network evolution. A single fiber core is necessary to be a quantum channel, due to the SNR requirement. The nonlinear effects of fiber, for example Raman scatting, will lead to a disastrous SNR when the bright light for communication and the quantum signal are transmitted in a single fiber. In short distance, continuous variable QKD scheme may be a usable countermeasure to resist noise interference. However, the real effective scheme to work properly under practical SNR has not emerged yet. The free space channel needs directly visible light path, the good atmospheric condition, and the acceptable SNR, which denotes the valid work time is severely limited.

### 4.3 Policies, legal and other non-technical obstacles

Cryptography is a strictly controlled technology in all countries. The evaluation and certification must be executed by a special government department following a standardization procedure. The certification is also necessary for business customers to make use of quantum cryptography. A lot of theoretical and experimental works must be achieved to establish the standard for production, security estimation and application of quantum cryptography. Besides, to find the balance between security protection and security control is not only the technical problem for academia, but also for policy makers of the government.

It is difficult for conventional crypto venders to confirm quantum cryptography. Most of the classical cryptographers do not really understand quantum mechanics and have no confidence in quantum cryptography (Lo, 1999). Moreover, some of them are hostile to quantum computation and quantum cryptography, since many classical productions will be no longer in force if these technology become veritable. The benefit alteration will cause a lot of resistance. The new growth points should be vigorously exploited rather than make division from the existing market.

## 5. Conclusion and future trends

In this chapter we surveyed the concept, security and realization of quantum cryptography, which has huge potentials to achieve physical security. Quantum cryptography is a revolutionary cryptographic technology, which has attracted the attention of various counties over either industrial or academic community. Although great achievements have been achieved in the past 20 years, there are still a lot of real-life difficulties must be overcome. At the end of the chapter, we would like to shortly infer some future evolutionary trends of quantum cryptography.

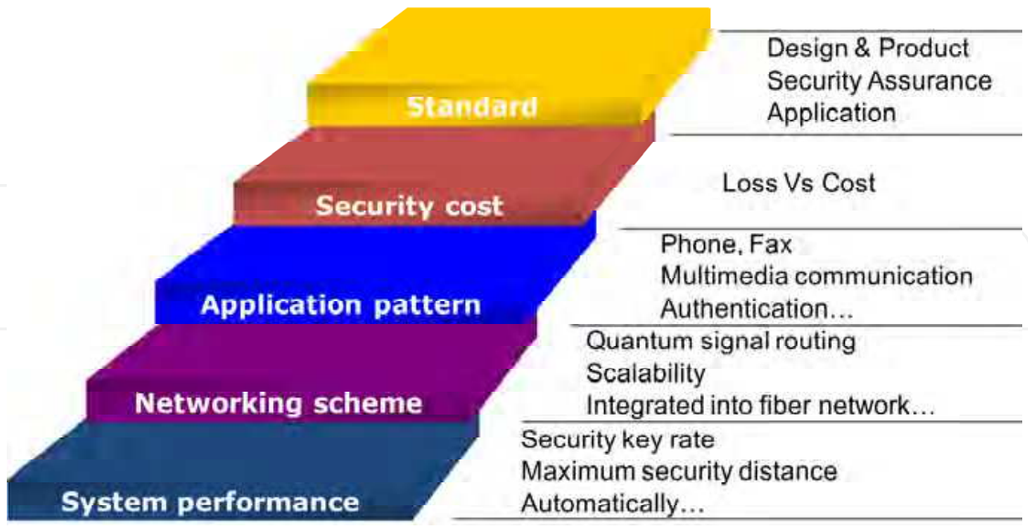



Fig. 17. The road to real-life QKD

Several stages on the road to real-life QKD are shown in Fig. 17. As the prime value, the security loopholes of real-life quantum cryptography system won't be too careful to be assessed. The key generation rate will be nonsense if the security of the procedure can not be

guaranteed. This project requires the joint efforts of many people from different areas such as scientists, engineers and users. Especially, quantum hackers are necessary to make quantum cryptography more reliable, while the persuasion to develop QKD rather than destroy it should be kept in mind. The root of the quantum hacking is that we use the untrusted classical devices to perform the practical QKD system, thus how to establish the standard of various devices is very important in future research of the security of practical QKD systems.

To improve the key distribution rate is still an important aspect of futer research, even if the QKD system which can generate Mbps secury key stream over 50 Km fiber channel has been demonstrated (Dixon, et al., 2008). The development step maybe retarded due to the performance limitation of SPD, modulation, post procession, and so on. The next hot research area will be in engineering field rather than physical area, aiming at making the effective and economic QKD equipment to be integrated into existing security infrastructure.

Networking is a nature evolution way of QKD. The infrastructure of large scale QKD networks is still immature. The quantum repeater to extend the secure transmission distance, the technolgy to integrate QKD network into exsisting optical communication network will be the hot research field. The real quantum cryptography network, in which the end users can use it in their real-life information transfer applications will be the next milestone.

At last, as the core of industry, standards for security evaluation, the production, and the application of QKD are already in development (ETSI, 2011) and will continuously attract the attention of researchers.

## 6. References

Bennett C. H, & Brassard, G. (1984). Quantum cryptography: Public-key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175 - 179.Bangalore, India, December 1984

Bennett C. H.; Bessette F.; Brassard G.; Salvail L. & Smolin J. (1992), Experimental quantum cryptography, *Jour. of Cryptology*, 5(1):3-28.1992.

Berta,M.; Colbeck, M. R.; Renes, J. M.; & Renner, R. (2010) The uncertainty principle in the presence of quantum memory, *Nature Physics*, Vol. 6. Issue 9, 659, 2010

Clauser, J. F.; Horne, Ma.; Shimony, A., Holt, R. A. (1969). Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.*, 23, 880-884, 1969

Chen, W.; Han, Z.-F.; Yin, Z.-Q.; Wu, Q.-L.; Wei, G. & Guo, G.-C. (2007). Decoy state quantum key distribution in telecom dark fiber, *Proceedings of the SPIE*, Vol. 6827, 682709-1-6, 2007

Chen, W.; Han. Z.-F.; Xu, F.-X.; Mo, X.-F.; Wei, G. & Guo, G.C. (2008). Active phase compensation of quantum key distribution system, *Chinese Science Bulletin*. Vol. 53, 1310-1314, 2008

Chen, W.; et al., (2009). Field experiment on a "star type" metropolitan quantum key distribution network, *IEEE Photonics Technology Letters*, Vol. 21, 575-577, 2009.

Chen, T.-Y.; et al., (2010) Metropolitan all-pass and inter-city quantum communication network, *Optics Express.* Vol. 18, Issue 26, pp. 27217-27225, 2010

Choi,I.; Young, R.J. & Townsend, P.D. (2010). Quantum key distribution on a 10Gb/s WDM PON, *Optics Express,* Vol. 18, No. 9, 2010

Deo, N. (1974). Graph Theory with Applications to Engineering and Computer Science (Prentice-Hall, 1974), pp. 33–34. theorems 2–8

Diffie W. & Hellman M. E. (1976). New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol. IT-22, pp. 644–654, 1976

Dixon, A.-R.; Yuan, Z.-L.; Dynes, J.-F.; Sharpe, A. W. & Shields, A. J. (2008). Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate, *Optics Express,* Vol. 16, Issue 23, pp. 18790-18979, 2008

Elliott, C.; Colvin, A.; Pearson, D.; Pikalo, O.; Schlafer, J.& Yeh, H. (2006). Current status of the DARPA quantum network,*Proc. of the SPIE,* Vol. 6372, pp. U270-U275, 2006

ETSI (2011). http://www.etsi.org/WebSite/Technologies/QKD.aspx

Fernandez, V.; Collins, R.J.; Gordon, K.J.; Townsend, P.D. & Buller, G.S. (2007). Passive optical network approach to gigahertz-clocked multiuser quantum key distribution, *IEEE J. Quantum Electron.* Vol. 43, No. 2, pp. 130-138, 2007

Gobby, C.; Yuan, Z. L. & Shields, A. J. (2004). Quantum key distribution over 122 km of standard telecom fiber, *Appl. Phys. Letts*. Vol. 84, Issue 19, 2004

Gottesman, D.; Lo, H.-K.; Lukenhaus, N. & Preskill, J.(2004). Security of quantum key distribution with imperfect devices, *Quantum Information and Computation,* Vol. 4, 325, 2004

Han, Z.-F.; Mo, X.-F., Gui, Y.-Z. & Guo, G.C., (2005). Stability of phase-modulated quantum key distribution systems, *Applied. Physics. Letters*, 86, 221103, 2005

Horodecki, K.; Pankowski, L.; Horodecki, M. & Horodecki, P. (2008). Low-dimensional bound entanglement with one-way distillable cryptographic key, *IEEE Trans. on Infor. Theory*, Vol. 54, Issue 6, p 2604-2620, 2008.

Hughes, R. & Nordholt, J. (2011). Refining Quantum Cryptography, *Science*, Vol. 333, 1584-1586, 2011.

Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* 91, 057901, 2003.

Kraus, B.; Gisin, N. & Renner, R. (2005). Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication, *Phys. Rev. Lett.* 95, 080501, 2005

Kumavor, P. D.; Beal, A. C.; Donkor, E. & Wang, B. C. (2006). Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture, *IEEE J. Light Tech.* Vol. 24, pp. 3103-3106, 2006

Li, H-W. Yin, Z.-Q.; Han, Z.-F.; Bao, W.-S. & Guo, G. C. (2010). Security of practical phase-coding quantum key distribution, *Quantum Information and Computation*, Vol. 10, No. 9 & 10 0771–0779, 2010

Li, H.-W.; Yin, Z.-Q.; Han, Z.-F.; Bao, W.-S. & Guo, G. C. (2011). Security of quantum key distribution with state-dependent imperfections, *Quantum Information and Computation*, Vol. 11, No. 11 & 12 0937–0947, 2011

Liu Y.; Chen, T.-Y.; Wang, J.; et al. (2010). Decoy-state quantum key distribution with polarized photons over 200 km, *Opt. Express*. 18(8):8587-94, 2010.

Lo, H.-K. (1999). Will Quantum Cryptography ever become a successful technology in the marketplace?, arXiv:quant-ph/9912011v1, 1999

Lo, H.-K.; & Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances, *Science* 283, 5410, 1999.

Lo, H.-K.; Ma, X.-F., & Chen, K. (2005). Decoy state quantum key distribution, *Phys. Rev. Lett.* 94, 230504, 2005.

Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.& Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination, *Nature Photonics* 4 686-689., 2010

Ma, L.-J.; Mink, A.; Xu, H.; Slattery, O. & Tang, X. (2007). Experimental demonstration of an active quantum key distribution network with over gbps clock synchronization, *IEEE Communications Letters*, Vol. 11, No. 12, 1019 -1021, 2007

Ma, L.-J.; et al., (2008). Experimental demonstration of a detection-time-bin-shift polarization encoding quantum key distribution system, *IEEE Comm. Lett.,* Vol. 12, No. 6, 2008.

Mo, X.-F.; Zhu, B.; Han, Z.-F.; Gui, Y.-Z. & Guo, G. C. (2005). Faraday–Michelson system for quantum cryptography, *Optics Letters*, Vol. 30, No. 19, pp.2632-2634, 2005.

Nishioka, T.; Ishizuka, H.; Hasegawa, T.& Abe, J. (2002). "Circular type" quantum key distribution, *IEEE Photonics Technology Letters,* Vol. 14, No. 4 , pp. 576-578, 2002

Pawlowski, M.; & Brukner, C. (2009). Monogamy of Bell's inequality violations in nonsignaling theories, *Phys. Rev. Lett.*, 102, 030403, 2009

Peev, M.; Pacher, C.; Alleaume, R.; et al. (2009). The SECOQC quantum key distribution network in Vienna, *New Jour. Of Phys.,* Vol. 11, 075001, 2009

Rarity, J. G.; Tapster, P. R.; Gorman, O.M. & Knight P. (2002). Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, 4. 82.1–82.21, 2002.

Renes, J. M. & Smith, G. (2007). Noisy processing and distillation of private quantum states, *Phys. Rev. Lett.* 98, 020502, 2007

Renner, R.; Gisin, N. & Kraus, B. (2005), Information-theoretic security proof for quantum-key-distribution protocols, *Phys. Rev. A*. 72,012332, 2005

Renner, R. (2005), PhD thesis, ETH No 16242, 2005 *http://quant-ph/0512258, 2005.*

Ribordy, G.; Gautier, J.-D.; Gisin, N.; Guinnard, O. & Zibinden, H. (1998). Automated "Plug &Play" quantum key distribution, *Electronics. Letters.* 34, (22), pp. 2116 - 2117, 1998

Rosenberg, D.; Peterson, C.G.; Harrington, J. W.; Rice, P. R., Dallmann, N., Tyagi, K. T., McCabe, K. P.; Nam S.; Baek, B.; Hadfield, R. H.; Hughes, R. J. & Nordholt J. E. (2009). Practical long-distance quantum key distribution system using decoy levels, *New Jour. of Phys.* 11, 045009, 2009.

Sasaki, M; et al., (2011). Field test of quantum key distribution in the Tokyo QKD Network, *Optics Express,* Vol. 9, Issue 11, pp. 10387-10409, 2011.

Scarani, V. & Gisin,N. Quantum communication between N partners and Bell's inequalities, *Phys. Rev. Lett*, Vol. 87, No.11, 117901,2001

Schmitt-Manderbach, T.; Weier, H.; Fürst, M.; Ursin, R.; Tiefenbacher, F.; Scheidl, T.; Perdigues, J.; Sodnik., Z.; Kurtsiefer, C.; Rarity, J.G.; Zeilinger, A & Weinfurter, H. (2007). Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, *Phys. Rev. Lett. 9*8, 010504 (2007)

Shannon, C. (1949). *Bell System Technical Journal* 28 (4): 656–715, 1949.

Shor, W.; Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol , *Phys. Rev. Lett.,* 85, pp.441-444, 2000.

Stucki D.; Walenta, N.; Vannel, F.; Thew, R. T.; Gisin, N.; Zbinden, H.; Gray. S.; Towery, C. R &Ten, S. (2009). High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres, *New Jour. of Phys.* 11, 075003, 2009.

Takesue, H.; Nam, S. W.; Zhang, Q., Hadfield, R. H.; Honjo, T.; Tamaki, K. & Yamamoto, Y. (2007). Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, *Nature Photonics,* 1, 343 – 348, 2007

Tomamichel, M.; Renner, R. (2011). Uncertainty relation for smooth entropies, *Phys. Rev. Lett.,* 106, 110506, 2011.

Townsend, P.D.; Phoenix, S.; Blow, K.J. & Barnett, S. (1994). Design of quantum cryptography systems for passive optical networks, *Electronic Letters*. 30 , 1875, 1994

Townsend, P.D. (1997). Quantum cryptography on multiuser optical fibre networks, *Nature,* 385, 47, 1997

Wang, X.-B. (2005). Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* 94, 230503, 2005

Wang, S.; et al., (2010). Field test of wavelength-saving quantum key distribution network , *Optics Letters*, Vol. 35 Issue 14, pp.2454-2456, 2010

Weier, H.; Krauss, H.; Rau, M.; Furst, M.; Nauerth, S.& Weinfurter, H. (2011). Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors, *New Jour. of Phys.* 13, 073024, 2011

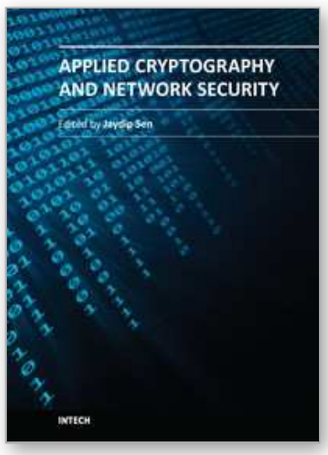
Wiesner, S, (1083), Congjugate coding, *SIGACT news*, 15(1):78-88, 1983

Xu, F.-X.; et al., (2009). Field experiment on a robust hierarchical metropolitan quantum cryptography network, *Chinese Science Bulletin*, Vol. 54, 2991-2997, 2009.

Xu, F.-H.; Qi, B. & Lo, H.-K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, *New Jour. of Phys*, 12, 113026, 2010

Zhang, L.-J.; Wang, Y.-G.; Yin, Z.-Q.; Chen, W.; Yang, Y.; Zhang, T.; Huang, D.-J.; Wang, S.; Li, F.-Y. & Han, Z.-F. (2011) Real-time compensation of phase drift for phase-encoded quantum key distribution systems, *Chin. Sci. Bull.*, Vol 56, 2305-2311, 2011

Zhang, Tao.; Mo, X.-F.; Han, Z.-F. & Guo, G.-C. (2008). Extensible router for a quantum key distribution network et al., *Phys Lett. A*., Vol.372, 3957-3962, 2008




**Applied Cryptography and Network Security**

Edited by Dr. Jaydip Sen

ISBN 978-953-51-0218-2
Hard cover, 376 pages
**Publisher** InTech
**Published online** 14, March, 2012
**Published in print edition** March, 2012

Cryptography will continue to play important roles in developing of new security solutions which will be in great demand with the advent of high-speed next-generation communication systems and networks. This book discusses some of the critical security challenges faced by today's computing world and provides insights to possible mechanisms to defend against these attacks. The book contains sixteen chapters which deal with security and privacy issues in computing and communication networks, quantum cryptography and the evolutionary concepts of cryptography and their applications like chaos-based cryptography and DNA cryptography. It will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.



INTECH
open science | open minds

**InTech Europe**
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

**InTech China**
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen